CLAIMS

What is claimed is:

1. A method for enabling secure communication between a client on an open network and a server apparatus on a secure network, the method performed on a intermediary apparatus coupled to the secure network and the open network, comprising:

negotiating a secure communications session with the client apparatus via the open network;

negotiating an open communications session with the server via the secure network;

receiving encrypted packet application data having a length greater than a packet length via multiple data packets;

decrypting the encrypted packet application data in each data packet;

forwarding decrypted, unauthenticated application data to the server via the secure network; and

authenticating the decrypted packet data on receipt of a final packet of the segment.

2. The method of claim 1 wherein said step of forwarding includes:

forwarding data which spans over multiple TCP segments.

3. The method of claim 2 wherein said data is not buffered during decryption.

4 The method of claim 2 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

5. The method of claim 2 wherein said step of forwarding includes authenticating the decrypted data after a final segment of a multi-segment encrypted data stream is received.

6. The method of claim 5 further including the step of notifying the client apparatus if a failure in said step of authenticating occurs.

7. A method for processing encrypted data transferred between a first system and a second system, comprising:

providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network;

receiving encrypted data from the first system via the open network in the form of application data spanning multiple packets, each packet having a packet length and information for authenticating the application data;

decrypting ones of said packets as said packets are received;

forwarding application data as said packets are decrypted to the second device via the secure network; and

authenticating the data when said information for authenticating the data is received in a last of said multiple packets.

8. The method of claim 7 wherein said step of receiving comprises receiving SSL encrypted data.

9. The method of claim 7 wherein said step of decrypting comprises decrypting application data encrypted using SSL and a DES algorithm.

10. The method of claim 7 wherein said step of decrypting is performed without buffering the encrypted data prior to decrypting the data.

11. The method of claim 7 further including the step, prior to said step of decrypting, of:

buffering blocks of said encrypted data for decryption.

12. The method of claim 11 wherein said step of buffering comprises buffering the data for a length sufficient to perform complete a block cipher used to encrypt the data.

13. The method of claim 12 wherein said block cipher is a form of DES.

14. The method of claim 7 wherein said step of authenticating includes a step of alerting the first device if said step of authenticating fails.

15. The method of claim 7 wherein said step of authenticating includes generating a reset to the second device is said step of authenticating fails.

16. A method of providing secure communications using limited buffer memory in an secure sockets layer processing device, comprising:

receiving SSL encrypted data having a length greater than a TCP segment carrying said data;

buffering the SSL encrypted data in a memory buffer in the SSL accelerator device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher;

decrypting the buffered segment of the received SSL encrypted data to provide decrypted application data; and

forwarding the decrypted application data to a destination device.

17. The method of claim 16 wherein the block cipher is 3DES.

18. The method of claim 16 wherein the block cipher is DES.

19. The method of claim 16 further including the step of authenticating the data on receipt of a final segment.

20. The method of claim 19 further including the step of generating an alert if said step of authenticating results in a failure.